



CVE-2008-5719

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2008-5719
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-26 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cross-site scripting (XSS) vulnerability in Hitachi Groupmax Web Workflow SDK Set for Active Server Pages before 06-52-

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hitachi	Groupmax Web Workflow Sdk Set For Active Server Pages	03-10	All	All	All

[illegible]

Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-10	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-10_a	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-11	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-11_a	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-20	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	05-20_a	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-00	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-01	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-02	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-03	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-03_a	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-50	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	06-51	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	3-10	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	3-10_a	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	3-10_b	All	All	All
Application	Hitachi	Groupmax Workflow To Development Kit For Active Server Pages	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References
Reference
Vulnerability in the Cross-site Scripting of Groupmax Workflow - Development Kit for Active Server Pages: Software Vulnerability Information:
Hitachi GroupMax Workflow Development Kit Cross-Site Scripting Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Groupmax Workflow Development Kit for Active Server Pages Cross Site Scripting Vulnerability
Groupmax Input Validation Flaw in Groupmax Workflow Development Kit for Active Server Pages Permits Cross-Site Scripting Attacks - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)